



CVE-2016-9463

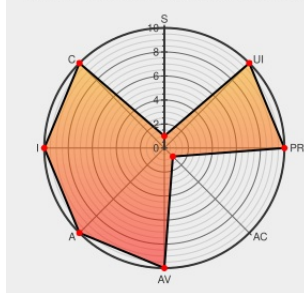
Published on: 03/27/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:18 PM UTC

CVE-2016-9463

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Nextcloud Server](#) from [Nextcloud](#) contain the following vulnerability:

Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.1.2, 9.0.6, and 8.2.9 suffer from SMB User Authentication Bypass. Nextcloud/ownCloud include an optional and not by default enabled SMB authentication component that allows authenticating users against an SMB server. This backend is implemented in a way that tries to connect to a SMB server and if that succeeded consider the user logged-in. The backend did not properly take into account SMB servers that have any kind of anonymous auth configured. This is the default on SMB servers nowadays and allows an unauthenticated attacker to gain access to an account without valid credentials. Note: The SMB backend is disabled by default and requires manual configuration in the Nextcloud/ownCloud config file. If you have not configured the SMB backend then you're not affected by this vulnerability.

CVE-2016-9463 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisories – ownCloud	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 owncloud.org/security/advisory/?id=oc-sa-2016-017
#148151 SMB User Authentication Bypass and Persistence - HackerOne	Exploit Third Party Advisory hackerone.com text/html	 hackerone.com/reports/148151
Merge pull request #2198 from owncloud/smb-auth-fix · owncloud/apps@5d47e7b · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 github.com/owncloud/apps/commit/5d47e7b52646cf79edadd78ce10c754290cbb732
Double verify the SMB response · nextcloud/apps@b85ace6 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 github.com/nextcloud/apps/commit/b85ace6840b8a6704641086bc3b8eb8e81cb2274
advisory – Nextcloud	Patch Vendor Advisory nextcloud.com text/html	 nextcloud.com/security/advisory/?id=nc-sa-2016-006
Operation OwnedCloud: Exploitation and Post-exploitation Persistence - Rhino Security Labs	Exploit Technical Description Third Party Advisory rhinosecuritylabs.com text/html	 rhinosecuritylabs.com/2016/10/operation-ownedcloud-exploitation-post-exploitation-persistence/
Double verify the SMB response · nextcloud/apps@dec91f · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 github.com/nextcloud/apps/commit/dec91fd31f4ffab191cbf09ce4e5c55c67a4087
[stable9] Merge pull request #2198 from owncloud/smb-auth-fix · owncloud/apps@16bccf · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 github.com/owncloud/apps/commit/16bccfc946c8711721fa684d78135ca1fb64791
[stable8.2] Merge pull request #2198 from owncloud/smb-auth-fix · owncloud/apps@a0e07b7 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 github.com/owncloud/apps/commit/a0e07b7ddd5a5fd850a6e07f8457d05b76a300b3

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Nextcloud Server	All	All	All	All
Application	Nextcloud	Nextcloud Server	All	All	All	All
Application	Owncloud	Owncloud	All	All	All	All
Application	Owncloud	Owncloud	All	All	All	All

```
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:*:
```

```
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:
```

```
cpe:2.3:a:owncloud:owncloud:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:owncloud:owncloud.*.*.*.*.*.*.*.*.*.*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report